What Is Claimed Is:

1. A method, comprising:

a) transmitting and receiving data with a second device via a first communication link to a first device to establish an identity of the first device; and

b) using the established identity for authentication of communications from the first device received by the second device via a second communication link.

2. The method of claim 1, further comprising transferring the established identity to the second communication link.

3. The method of claim 1, further comprising:

sending a nonce to the first device via the first communication link; and

receiving at the second device at least one of the nonce and a function of the nonce from the first device via the second communication link.

4. The method of claim 3, further comprising encrypting the nonce at the second device for the first device.

5. The method of claim 1, further comprising:

receiving a nonce at the first device via the first communication link; and

sending at least one of the nonce and a function of the nonce from the first device via the second communication link.

6. The method of claim 1, further comprising:

determining an optimal communication link from a plurality of communications links between the first device and second device; and

using the established identity for communication between the first device and the second device via the optimal communication link.

7. The method of claim 1, further comprising:

periodically sending a nonce from the second device via the first communication link to the first device; and

maintaining the second communication link with the first device only if a response to the nonce is received from the first device via the second communication link.

8. The method of claim 1, wherein b) comprises:

determining an address of the first device; and

authenticating communications received from the address as being from the first device.

9. The method of claim 1, wherein b) comprises:

transmitting security credentials from the second device to the first device via the first communications link; and

identifying communications that utilize the security credentials received at the second device over the second communications link as being from the same first device.

10. The method of claim 9, further comprising:

receiving the security credentials at the first device;

encrypting data using the security credentials; and

sending the encrypted data via the second communications link.

11. The method of claim 9, further comprising decrypting encrypted data received via the second communications link at the second device in order to identify the first device.

12. A machine readable medium that provides instructions, when executed by a computing platform, cause said computing platform to perform operations comprising a method of:

transmitting and receiving data with a server via a first communication link to a client to establish an identity of the client; and

using the established identity for authentication of communications from the client received by the server via a second communication link between the client and the server.

13. The machine readable medium of claim 12, further comprising instructions, which when executed by a computing platform, cause said computing platform to perform further operations of:

sending a nonce to the client via the first communication link; and

receiving at the server at least one of the nonce and a function of the nonce from the client via the second communication link.

14. The machine readable medium of claim 13, further instructions, which when executed by a computing platform, cause said computing platform to perform further operation of perform encrypting the nonce for the client.

15. The machine readable medium of claim 12, further comprising instructions, which when executed by a computing platform, cause said computing platform to perform further operations of:

determining an optimal communication link from a plurality of communications links between the client and server; and

using the established identity for communication between the client and the server via the optimal communication link.

16. The machine readable medium of claim 12, further instructions, which when executed by a computing platform, cause said computing platform to perform further operations of:

periodically sending a nonce via the first communication link to the client; and

maintaining the second communication link with the client only if a response to the nonce is received from the client via the second communication link.

17. The machine readable medium of claim 12, further comprising instructions, which when executed by a computing platform, cause said computing platform to perform further operations of:

determining an address of the client; and

authenticating communications received from the address as being from the client.

18. The machine readable medium of claim 12, further comprising instructions, which when

executed by a computing platform, cause said computing platform to perform further operations of:

transmitting security credentials from the server to a client via the first communications link; and

identifying communications that utilize the security credentials received at the server over the second communications link as being from the same client.

19. The machine readable medium of claim 21, further comprising instructions, which when executed by a computing platform, cause said computing platform to perform further operation of decrypting encrypted data from the client at the server in order to identify the client.

20. An apparatus comprising:

a first module adapted to establish an identity of a client device to a server via at least a first communications link; and

a second module adapted to authenticate the client device on another communications link based on the established identity.

21. The apparatus of claim 20, wherein the first communications links is authenticatable.

22. The apparatus of claim 20, wherein the other communications link is unauthenticatable.

23. The apparatus of claim 20, wherein the second module comprises a driver adapted to send a nonce to the client device via the first communication link and to receive the nonce or a function of the nonce from the client device via the other communication link.

24. The apparatus of claim 23, wherein the second module comprises a second driver adapted to receive a nonce at the client device via the first one of the communication links and to send the nonce or a function of the nonce to the server via the other of the communication link.

25. A machine readable medium that provides instructions, when executed by a computing platform, cause said computing platform to perform operations comprising a method of:

transmitting and receiving data with a client via a first communication link to a server to establish an identity of the client; and

transmitting and receiving data with the client via a second communication link between the client and the server using the established identity.

26. The machine readable medium of claim 25, further comprising instructions, which when executed by a computing platform, cause said computing platform to perform further operations of:

receiving a nonce at the client via the first communication link; and

sending at least one of the nonce and a function of the nonce to the server via the second communication link.

27. The machine readable medium of claim 25, further instructions, which when executed by a computing platform, cause said computing platform to perform further operations of:

periodically receiving at the client a nonce sent via the first communication link from the server; and

sending a response to the nonce from the client to the server via the second communication link.

28. The machine readable medium of claim 25, further instructions, which when executed by a computing platform, cause said computing platform to perform further operations of:

receiving security credentials at the client;

encrypting data at the client using the security credentials; and

sending the encrypted data to the server via the second communications link.